Introduction ***PRELIMINARY***.

Information has four dimensions of value: operational, individual, societal, and value to others (Gillies, 2011). From an operational value approach, information is considered an asset to an organization which must be protected to maintain efficiency and effectiveness. Maintaining this information asset, an organization must mitigate the risks associated with the personal information stored about individuals and other organizations. To ensure individual value, information must be handled with due care, respect privacy concerns of those affected by the maintenance of the information asset, and meet expectations that the information is being safeguarded. If the information asset is compromised, the organization may be faced with a damaged reputation, changes in stock value, and litigation. Society, namely the stakeholders of an organization, also has an expectation of privacy and safety regarding information assets (Gillies). ***INSERT SOX FINES/PUNISHMENTS HERE.*** Unfortunately, information assets have value to others who do not have a legitimate purpose for the asset. If an organization fails to implement an effective and efficient IT security framework, this asset can be used to do harm.

As the global society has become reliant on IT as a means to exchange information from personal use of a computer to organizations and governments, IT security has become a concern for virtually everyone (Gillies, 2011). Hacks, cyberattacks, and information compromises and losses from organizations and the government have resulted in legislation that requires IT security practices, processes, and procedures be implemented to protect information assets and preserve values of information (Gillies). Organizations struggle with the interpretation and implementation of legislated IT security standards and may turn to outside security consultants as means to protect information assets; however, attacks on the asset still continue (Gikas, 2010).

ISO 27000

The ISO family of standards revolve around the “plan-do-check-act” (PDCA) cycle (Gillies, 2011), a process approach (Gikas, 2010). The cycle is attributed to Shewhart in 1939 through his statistical process improvement research at Bell Laboratories (Gillies). ***INSERT INFO ABOUT SHEWHART AND DEMINGS HERE.*** ISO 27001, established in October 2005 (Gikas, 2010) “establishes, implements, operates, monitors, reviews, and improves and Information Security Management System (ISMS) through a framework or model (Gillies, 2011) in reference to an organization’s overall business risks (Gikas, 2010). ISO 27000 replaced the BS7799-2 standard, published in the 1990s (Gikas). ISO 27001, which emerged from BS77992- and grants certification (Gikas), assumes that if the framework process is operating effectively and efficiently, the resulting outcome regarding IT security will be acceptable (Gillies, 2011). ISO 27001 is an international standard that can be employed by any organization such as corporations, government agencies, and not for profit entities, that implements IT security control customized to the needs of the specific organization and information assets the organization maintains (Gikas, 2010). The organization’s goals, security needs, operating processes, size, and structure must be taken into consideration upon planning for the design and implementation of ISO 27001 through the use of the PDCA cycle (Gikas). The PCDA cycle aims to make certain that adequate and appropriate IT security controls are present to protect the information assets and increase public confidence in the safeguard of these assets and addresses confidentiality, integrity, and availability characteristics of the IT system and information assets as well as both physical and nonphysical security procedures and practices (Gikas).

ISO 27002, formerly ISO 17799, is the standard of practice for security of information assets, and specifically instructs organizations how to implement the guidance in ISO 27001 (Gikas, 2010). ***INSERT ISO 27002 CONTROLS HERE.***

ISO 27003 outlines the PCDA cycle, its implementation, review, and improvement, and provides ISMS implementation guidance to organizations (Gikas, 2010).

ISO 27004, not yet published, is the new standard that will provide IT security management measurement and metrics (Gikas, 2010).

ISO 27005 focuses on IT security risk management (ISRM) and includes ISRM guidelines for organizations to comply with ISO 27001 ISMS (Gikas, 2010).

The certification standard, ISO 27006, outlines accreditation, certification, and registration for ISMS (Gikas, 2010).

Works Cited

Gikas, C. (2010). “A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards,” *Information Security Journal: A Global Perspective, 19, pp. 132-141.*

Gillies, A. (2011). “Improving the Quality of Information Security Management Systems with ISO 27000,” *The TQM Journal, Vol 23, Iss 4, pp. 367-376.*